TUMB 111

TITLE OF THE INVENTION

METHOD AND SYSTEM FOR FILTERING COMMUNICATION

PRIORITY CLAIM

This application is a continuation-in-part of U.S. Patent Application Number 09/967,117 which is a continuation of U.S. Patent Application Number 09/180,377, entitled "E-MAIL FIREWALL WITH STORED KEY ENCRYPTION/DECRYPTION," Now U.S. Patent Number 6,609,196 filed November 3, 1998, which is a national stage patent application filed under U.S.C. §371, based on PCT/US98/15552 entitled "E-MAIL FIREWALL WITH STORED KEY ENCRYPTION/ DECRYPTION," filed on July 23, 1998, which claims priority to U.S. Provisional Application Number 60/053,668, entitled "ELECTRONIC MAIL FIREWALL," filed July 24, 1997.

FIELD OF THE INVENTION

The present invention relates to communication systems, and more particularly to electronic message delivery.

BACKGROUND OF THE INVENTION

Receiving unwanted electronic messages, such as e-mail, wastes time and valuable resources. Electronic message communication has become a prevalent, and perhaps preferred, method of communication. Such communication is apparent in most aspects of daily life including the workplace, the home, and even the road. At the workplace, the messages may arrive from clients, partners, customers, or other employees. Additionally, unwanted messages, for example "SPAM" messages, are received by users. The circumstances are similar for the home user where both wanted and unwanted messages are received. Reviewing the unwanted

messages consumes time, which may be highly valuable in the case of workplace time, and may also undermine the user's capacity to receive other, desirable, messages. Moreover, the unwanted messages may be messages including computer viruses or other malicious code which may harm the user's system. Accordingly, there is a need for a method that controls and restricts reception of unwanted or harmful messages.

SUMMARY OF THE INVENTION

Therefore, in accordance with the invention, a method is presented for reducing the number of harmful messages received by users of a protected e-mail network. The method includes providing an e-mail relay, or firewall, between the e-mail network and the public network to scan incoming messages intended for local recipients of a computer network. The e-mail relay detects signature data in incoming e-mails. The e-mail relay extracts the signature data from an e-mail. The e-mail relay validates and optionally classifies the signature data. If the verification or classification result is acceptable, the e-mail relay allows the message to proceed to at least one intended recipient.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 illustrates a network arrangement, which includes a e-mail relay, in accordance with the invention; and

Figure 2 is a flow diagram illustrating a method for reducing the number of harmful messages received by an enterprise in the network configuration of Figure 1.

DETAILED DESCRIPTION OF THE INVENTION

The invention is discussed by reference to figures illustrating the structure and operation of an example system. First, the logical structure of a network arrangement according to the

invention is described. Next, the operation of the e-mail relay of the network arrangement when examining incoming e-mails is discussed by reference to a flow diagram.

The structure of a network, in which a reduced number of harmful messages are received by users of the protected enterprise, will now be discussed with reference to Figure 1. Although, the discussion below refers to the protected network resources as part of an enterprise, protected resources of the invention additionally include other types of organizations and network resources such as internet service providers and corresponding subscribers and an Internet webmail site protecting user accounts. The illustrated network arrangement includes user stations 34, 36, an e-mail server 40, a public network 44, and an email relay 46 in accordance with the invention. The user stations 34, 36, and the e-mail server 40 are coupled together by a network such as a Local Area Network (LAN). The network is used to internally couple enterprise resources in a generally trusted manner since the network is preferably separated from the external, or public, network 44 by an access firewall (not shown). The access firewall is discussed only for purposes of explanation and is not required for operation of embodiments employing the principles of the present invention. The public network 44 is preferably a Wide Area Network (WAN) such as the Internet. The public network 44 facilitates communication of messages to the local network.

The e-mail relay 46 is preferably interposed behind the common access firewall, on the "safe side" of the access firewall. The e-mail relay 46 advantageously takes a form as described in further detail herein to filter messages received from outside the protected enterprise. Preferably, the e-mail relay 46 takes the form of a program executing on a conventional general purpose computer. In one embodiment, the computer executes the Windows NT or Windows 2000 operating systems available from Microsoft Corp., of Redmond, Washington. In other

embodiments, the computer executes a Unix operating system such as Solaris from Sun Microsystems, of Mountain View, California. In some embodiments, the e-mail relay 46 includes processes and data distributed across several computer systems, which are logically operating as a single e-mail relay in accordance with the invention. Although the e-mail relay 46 is shown as operating on messages between an internal site and an external site, the e-mail relay 46 may also be used to filter messages between two internal sites. Furthermore, the e-mail relay 46 can be used to filter outgoing messages, such as those, for example, from a hacker employing the enterprise resources to transmit harmful messages.

The email relay 46 is coupled to an e-mail server 40 associated with the enterprise 32. The e-mail server 40 preferably facilitates processing of messages by local user stations 34, 36. In one embodiment, the e-mail server 40 is configured as a Simple Mail Transfer Protocol (SMTP) server. An example e-mail server is a Microsoft Exchange Server from Microsoft Corp. As may be appreciated, the e-mail server 40 is only one of the resources provided by the enterprise 32. The enterprise 32 usually includes various other resources to facilitate communication, administration, and other business tasks.

The e-mail relay 46 has available a validation authority module 37, which is used to examine signature data associated with messages. As is known, the e-mail relay 46 is also associated with data storage (not shown) for facilitating proper operation of various aspects of the e-mail relay.

As unknown sender system 28 is coupled to the public network 44 to transmit messages to recipients associated with the enterprise 32. As may be appreciated, in some instances, the unknown system 28 is composed of various combinations of resources and configuration different from those employed in the illustrated enterprise 32, as is known in the art.

Furthermore, the system 28 may employ various protocols to communicate with respective local stations.

The user stations 34, 36 are preferably user terminals, which are configured to facilitate business processes related to the enterprise's operation. In one embodiment, the user stations 34, 36 are computer systems at employee offices. The user stations 34, 36 are preferably coupled to the e-mail server 40 over the local area network to access e-mail applications.

The e-mail server 40 facilitates the transmission of messages between user stations 34, 36 and external systems. Messages intended for recipients within the enterprise are processed by the e-mail server 40 and are forwarded to the recipients by way of the local network. Messages intended for recipients outside the enterprise are processed by the e-mail server 40 and are transmitted over a communication link between the e-mail server and the public network 44. The public network 44 proceeds by facilitating delivery of the messages to the various intended recipients.

The present invention is based on the recognition that a sender's identity can be employed to properly characterize an message as either clean or potentially harmful. Specifically, when the identity of a sender can be verified and properly classified to match a desired security level, messages from that sender can be trusted as non-harmful.

Accordingly, the e-mail relay 46 operates to filter incoming messages so as to reduce the number of harmful messages received by the enterprise 32 by examining the sender's identity. Sender identity is communicated to the e-mail relay 46 by way of signature data associated with a message. As is know in the art, senders can attach signature data to transmitted messages in the form of a secure signature certificate, which authenticates the sender. Furthermore, the present status of a signature certificates, i.e., valid or invalid, may be publicly available. Hence

the e-mail relay can employ this public information, when available, to verify that a certificate has not been revoked. In one embodiment, the validation authority module 37 has available a revocation list, which is used to examine certificates' revocation status. In another embodiment, the validation authority module 37 employs a remote server to validate certificates.

In operation, local users are the target of communication from various entities coupled to the public network 44. In one embodiment, at least part of such communication is intercepted by the e-mail relay 46. For example, an outside sender of an message composes a message and transmits the message over the public network 44 to the enterprise. The email relay 46 intercepts the message instead of allowing it to proceed to the e-mail server 40, as is known in the art of store and forward protocol, such as SMTP. The e-mail relay 46 determines whether to forward the message to the e-mail server 40 after some inspection. The e-mail server 40 refers to the destination field of the message to identify the local recipient. The message is then transmitted to a user station associated with the local recipient if it has been determined that the sender is a trusted party. In another embodiment, the e-mail server 40 transmits the message to the user station only after the user requests the message. For example, e-mail servers executing the Post Office Protocol version 3 (POP3) or Internet Message Access Protocol (IMAP) operate in this manner when receiving messages for associated users.

Figure 2 illustrates a method employed by the e-mail relay 46 to filter harmful messages in the network arrangement of Figure 1. The e-mail relay 46 is generally adapted to filter e-mail received into the enterprise 32 by references to sender signature data included in messages. Particularly, the e-mail relay 46 validates and classifies signature data. The classification and validity status are employed to determine whether an message should be allowed to flow to the e-mail server 40 or should be diverted and subject to other action. Some of those actions, which

the e-mail relay 46 is adapted to execute, include: quarantine the e-mail in the local message store database 38, and reject the e-mail, while generating a special message to the intended recipient indicating that the message has been diverted.

The e-mail relay 46 operates to intercept messages and determine whether the e-mail includes signature data. Typically, the signature data is provided by an attachment certificate to the message. The e-mail relay 46 extracts signature data when signature data was detected (step 54). When signature data is not detected, the e-mail relay preferably delays delivery of the message until a determination that the message is not harmful has been reached by application of a policy (step 56) co-pending U.S. patent application No. discloses such application in the context of a SPAM policy. If signature data was extracted, it is validated preferably by employing the validation authority module 37.

In one embodiment, the e-mail relay 46 receives a message sender classification from the validation authority in response to submitting a certificate for validation. In other embodiments, classification is not employed by rather the message is processed only based on validity status. When employing classification, the e-mail relay assigns level of trust to senders based on stored information. For example, employees of the protected organization may receive the highest level, followed by vendors and customers.

As may be appreciated, the classification level for message acceptance may be set at different levels depending on system status. For example, at times when SPAM attacks are likely, the required classification level may be set higher to only allow highly trusted senders to pass without scrutiny.

Example policies that may be employed in a system of the invention include a policy that rejects all incoming messages with attached Microsoft WORD files including macro functions

unless the message was signed by a trusted party (for example, determined by reference to a trusted party directory). This same policy may further include a condition where messages with attached Microsoft WORD files without macros are accepted without further scrutiny. Other example policies include rejecting all executable attachments (signed or unsigned), rejecting all messages with attachments unless the message as well as the attachment were signed by a trusted party, reject all messages unless they were signed by a trusted organization (organization level signature), reject all messages including attachments unless they were signed by a trusted organization, quarantine all messages unless they were signed by a trusted party or organization unless a response message to an enrollment request was received from the sender.

Several example scenarios will now be discussed with reference to Figure 1. The example scenarios are not meant to limit the invention to any particular implementation or configuration but rather merely illustrate the various configurations and implementations which may be available in a system of the invention. Generally, the available configurations and processes refer to several attributes of an incoming message in determining an appropriate action applicable to the incoming message. The attributes include message content, attachment content, attachment presence, attachment type, sender type (individual, department, organization, domain), message content creator (individual, department, organization, domain). As discussed above, the available actions include reject, accept, quarantine, quarantine until signed, and validated (clean).

A system in accordance with the invention can be employed to screen outgoing message from within the protected enterprise 32. n this implementation the organization has a policy that requires all outgoing messages to be signed. A user employs a user station 36 to compose and sign an email by attaching a corresponding signature certificate to the message. The message is

received by the e-mail server 40. The e-mail server 40 routes the message to the intended external recipient (outside of the enterprise 32). The e-mail relay 46 intercepts the message. The e-mail relay 46 determines whether a signature is attached to the message. The e-mail relay 46 also determines whether the signature is valid by employing the validation authority 37. When the e-mail relay 46 receives confirmation that the signature is indeed valid, the message is allowed to pass to the public network 44 and to it's intended recipient.

If the e-mail relay 46 receives an message that does not include a signature, the e-mail relay generates a notification message for the sender. The notification message preferably communicates to the sender that the message was not transmitted to the intended external recipient because it failed to meet the requirements of the signing policy. The sender can then resend the message with the appropriate signature data.

The system of the present invention can also be used to allow external senders to properly send signed messages to recipient users of an enterprise. For example, an external sender composes and transmits an unsigned message to a recipient associated with the enterprise by way of the public network 44. The e-mail relay 46 intercepts the message arriving from the public network. The message is first examined to determine if it is a harmful message. If the e-mail message is determined to be clean, i.e., not harmful, the e-mail relay 46 determines whether the message is signed. When the e-mail relay 46 detects that the message is not signed, the e-mail relay generates an enrollment notification for the message recipient. The enrollment notification preferably communicates to the recipient that an unsigned message has been received for the recipient and the recipient should connect to the e-mail relay to generate a signature for the sender. The notification is received by the e-mail server 40 and is made available to the recipient. The recipient employs the user station 36 to connect to the e-mail relay 46 and

complete an enrollment request for the sender.

The enrollment preferably results in the generation of a private/public key pair as well in a signature certificate for the sender. The e-mail relay 46 preferably employs a publicly available registration authority to enroll the sender and generate a certificate for the sender including encryption and signature data. The e-mail relay 46 then sends an initial user ID and password so as to allow the sender to access the e-mail relay 46 and retrieve the certificate which was generated for the sender. The sender connects to the e-mail relay 46 and composes an e-mail for the recipient by employing the sender's private key. The sender can also download the certificate data to the sender's computer when the sender wishes to employ his own computer to generate the signed messages rather than employ the e-mail relay for the signature application step.

Although the present invention was discussed in terms of certain preferred embodiments, the invention is not limited to such embodiments. A person of ordinary skill in the art will appreciate that numerous variations and combinations of the features set forth above can be utilized without departing from the present invention as set forth in the claims. Thus, the scope of the invention should not be limited by the preceding description but should be ascertained by reference to claims that follow.